

⑫ 公開特許公報(A)

平3-15886

⑮ Int. Cl.:

G 09 C 1/00
G 06 F 7/552
7/72

識別記号

A

庁内整理番号

7343-5B
7056-5B
7056-5B

⑬ 公開 平成3年(1991)1月24日

審査請求 未請求 請求項の数 2 (全6頁)

⑭ 発明の名称 べき乗剰余計算装置

⑯ 特 願 平1-149397

⑰ 出 願 平1(1989)6月14日

⑱ 発 明 者 高 林 京 子 神奈川県川崎市幸区小向東芝町1 株式会社東芝総合研究所内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 代 理 人 弁 理 士 三 好 秀 和 外1名

明 細 書

1. 発明の名称

べき乗剰余計算装置

2. 特許請求の範囲

(1) P, C, Dが入力データで、べき乗剰余計算 $C^D \bmod P$ を計算するべき乗剰余計算装置において、

$D' = (P-1) - D$ で表わされる D' を計算する手段と、 D もしくは D' を指数としたときの乗算回数 T_d 又は $T_{d'}$ を計算する手段と、 C と P が互いに素で前記乗算回数が $T_d > T_{d'}$ のときには $C^{D'} \bmod P$ の乗法的逆元を出力し、それ以外のときには $C^D \bmod P$ を出力する手段とを具備することを特徴とするべき乗剰余計算装置。

(2) 前記乗算回数を計算する手段は、指数 X を2進展開したときの X の桁数及び“1”の数から乗算回数を計算することを特徴とする請求項1に記載のべき乗剰余計算装置。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、処理桁数の大きなべき乗剰余計算に好適なべき乗剰余計算装置に関するものである。

(従来の技術)

公開鍵暗号方式の中で最も注目されているRSA暗号の復号化は、次式で示されるように、べき乗剰余計算を行って暗号文 C から平文 M を復号することにより以下のように行なわれる。

$$M = C^{D \bmod N}$$

ただし、 M : 平文 C : 暗号文 D : 秘密鍵 N : 2つの素数 P , Q の積

従来のRSA暗号の復号化方式としては、「RSA暗号の復号化装置」(特開昭63-129388)が知られている。

第4図は、この方式を説明するためのフローチャートである。この方式ではまず、入力データ C , 法 $N (= PQ)$, 指数 D , 法 N との最大公約数 $\gcd(C, N)$ が1かどうかを示すフラグ FLG を

初期設定する(ステップ401)。

次に、ステップ402でフラグFLGが「1」であると判別された場合には、指数 $D' = (P-1)(Q-1) - D$ を用いてべき乗剰余の計算を行った後(ステップ403)、その結果 M' の乗法的逆元 M を計算して、入力データCの復号結果とする(ステップ404)。

一方、ステップ402でフラグFLGが「1」以外の値であると判別された時は、指数Dを用いてべき乗剰余の計算をし、その結果を復号結果とする(ステップ405)。

この方式では、 D' のとり範囲がDと同じ $0 < D' < N$ で、 $\gcd(C, N) = 1$ の時は常に D' で計算するので、Dによってはかえって計算量が増加してしまうという問題があった。

(発明が解決しようとする課題)

以上述べたように、従来の方式は D' を用いてべき乗剰余計算をすると、Dで計算するよりも計算量が増加してしまう場合があるという欠点があった。

計算する場合、指数Dから $D' = (P-1) - D$ を計算し、Dと D' で計算量が少なくなる値を指数としてべき乗剰余計算を行うため、乗除算回数が減少し、高速にべき乗剰余計算を行うことができる。

更に、本発明とQuisquaterの方法を用いて、RSA暗号の復号化処理を行う場合、本発明を組み合わせてることにより、更に処理を高速に行うことができる。

(実施例)

以下、図面を参照して本発明の実施例を説明する。

具体的実施例の説明に入る前に、本発明の原理を以下に述べる。

$C^{D \bmod P}$ を計算する場合、CとPが互いに素の時は、 $D' = (P-1) - D$ をDの代わりに指数として用いてべき乗剰余計算をおこなっても同じ結果となる。これはフェルマーの小定理から導くことができる。

フェルマーの小定理とは、

従って、本発明ではDを用いてべき乗剰余計算をするよりも常に計算量が少なくなるべき乗剰余計算装置を提供することを目的とする。

(発明の構成)

(課題を解決するための手段)

この発明は、上記の目的を達成するために、P、C、Dが入力データで、べき乗剰余計算 $C^D \bmod P$ を計算するべき乗剰余計算装置において、 $D' = (P-1) - D$ で表わされる D' を計算する手段と、Dもしくは D' を指数としたときの乗算回数 T_d 又は $T_{d'}$ を計算する手段と、CとPが互いに素で前記乗算回数が $T_d > T_{d'}$ のときには $C^{D' \bmod P}$ の乗法的逆元を出力し、それ以外のときには $C^{D \bmod P}$ を出力する手段とを具備することを特徴とするものである。

特に、前記乗算回数を計算する手段としては、指数Xを2進展開したときのXの桁数及び「1」の数から乗算回数を計算するものが好ましい。

(作用)

本発明によれば、指数計算を素数Pのもとで

「Pが素数ならば、 $\gcd(a, p) = 1$ なるaに対して、常に

$$a^{P-1} \equiv 1 \pmod{p}$$

が成立する。」

である。

よって、 D' を指数としてフェルマーの小定理を用いると

$$\begin{aligned} M' &= C^{D' \bmod P} \\ &= C^{(P-1) - D \bmod P} \\ &= \frac{C^{P-1 \bmod P}}{C^{D \bmod P}} \bmod P \\ &= \frac{1}{C^{D \bmod P}} \bmod P \end{aligned}$$

続いて、 M' の乗法的逆元Mを求めて復号結果とする。乗法的逆元を求めるには、拡張ユークリッドの互除法を用いれば良い。

法Pは素数なので、 $0 < C < P$ ならば、入力データCと法Pは必ず互いに素となり、すべての入力データCに対して、本発明を適用することができる。

第1図は、第1の実施例における法を素数としたべき乗剰余計算装置の概要を示すブロック図である。

同図において、101は素数Pをセットするレジスタ、102は被べき乗数をセットするレジスタ、103は指数Dをセットするレジスタ、112は指数D' ($= (P-1) - D$) を計算する回路、104は指数D' をセットするレジスタである。

また、105は指数Dのときの乗除算回数Tdと指数D'のときの乗除算回数Td'を計算する回路、106は法と被べき乗数が互いに素で $Td > Td'$ であるときフラグ"1"を立てておくフラグレジスタである。

また、107はフラグレジスタに"1"が立っている場合にはレジスタ104の出力を選択し、"1"が立っていない場合にはレジスタ103の出力を選択するマルチプレクサである。

108は前記レジスタ101の出力値Pと前記レジスタ102の出力値Cと前記マルチプレクサ

107の出力値DまたはD'を入力として $C^X \bmod P$ ($X = D$ は又は、 D') を計算するべき乗剰余計算回路である。

109は前記フラグレジスタ106の値が"1"の時に前記べき乗剰余計算回路の出力値を後述する乗法的逆元計算回路側に出力し、それ以外の時は復号化出力側に出力するデマルチプレクサである。

また、110は前記フラグレジスタ106の値が"1"の時に、前記デマルチプレクサ109の出力値M'と前記レジスタ101の出力値Pを入力として、 $M' \cdot M' \equiv 1 \bmod P$ となるM'を計算する乗法的逆元計算回路、111はべき乗剰余計算装置全体を制御する制御回路である。

第2図は、第1の実施例の処理手順を示すフローチャートである。まず、入力データC、法P、指数D、指数D'、フラグを初期設定する(ステップ201)。

次に、フラグ1の場合には(ステップ20YES)、指数D'を用いたべき乗剰余の計算を行っ

た後(ステップ203)、その出力値M'の乗法的逆元M''の計算を実行して、このM''を復号結果とする(ステップ204)

一方、フラグが1でない時は(ステップ202NO)、指数Dを用いてべき乗剰余の計算を実行し、その出力値Mを復号結果とする(ステップ205)。

但し、 $D' = (P-1) - D$

フラグFLG = "0" ... 指数Dの乗除算回数 < 指数D'の乗除算回数

フラグFLG = "1" ... 指数Dの乗除算回数 > 指数D'の乗除算回数かつ、
 $\gcd(C, P) = 1$

次に、本発明の第2の実施例について説明する。これは、本発明をRSA暗号の復号処理に利用しようというものである。本発明とQuisquaterの方法を用いた復号アルゴリズムを以下に述べる。

Quisquaterの方法は公開鍵Nの素因数PとQを直接用いて復号処理を並列に計算する方法である。復号処理を行う人は秘密鍵Dを知っているの

で、秘密の素因数PとQを直接用いても安全性は低下しない。RSA暗号では、次式が成立する。

$$M = C^D \bmod N \\ N = PQ$$

ここでc1, c2, d1, d2, e1, e2を、

$$\begin{aligned} c1 &= C \bmod P \\ c2 &= C \bmod Q \\ d1 &= D \bmod P-1 \\ d2 &= D \bmod Q-1 \\ e1 &= M \bmod P \\ e2 &= M \bmod Q \end{aligned}$$

と定義すると、次式が成立することは明らかである。

$$\begin{aligned} e1 &= c1^{d1} \bmod p \\ e2 &= c2^{d2} \bmod q \\ e1, e2 &\text{が求まれば、} \\ M &\equiv e1 \pmod{p} \\ M &\equiv e2 \pmod{q} \end{aligned}$$

なので、中国剰余定理により連立合同式を解いてMが求まる。

次に、この方式と本発明を用いた高速復号法を説明する。

この方式に更に本発明を用いて、 d_1' 、 d_2' を

$$d_1' = (P-1) - d \pmod{p-1}$$

$$d_2' = (Q-1) - d \pmod{q-1}$$

$$a_1' = M^{d_1'} \pmod{p}$$

$$a_2' = M^{d_2'} \pmod{q}$$

と定義する。

次に、被乗数を c_1 、指数を d_1 としたときの乗除算回数 Td_1 、被乗数を c_1 、指数を d_1' としたときの乗除算回数 Td_1' 、被乗数を c_2 、指数を d_2 としたときの乗除算回数 Td_2 、被乗数を c_2 、指数を d_2' としたときの乗除算回数 Td_2' を計算する。

$Td_1 > Td_1'$ のときは d_1' を指数として、それ以外の時は d_1 を指数として用いて、べき乗剰余計算をする。 Td_2 、 Td_2' についても同様である。

もし d_1' 又は d_2' を用いてべき乗剰余計算

0は指数 d_1' をセットするレジスタ、311は指数 d_2 をセットするレジスタ、312は指数 d_2' をセットするレジスタである。

307は指数 d_1 、 d_1' 、 d_2 、 d_2' の2進展開したときの桁数と“1”の数から乗除算回数を計算する回路、308は法 Q と被べき乗数 c_2 とが互いに素で $Td_2 > Td_2'$ である時フラグ“1”を立てておくフラグレジスタである。

324は法 P と被べき乗数 c_1 とが互いに素で $Td_1 > Td_1'$ である時フラグ“1”を立てておくフラグレジスタである。

313は前記レジスタ309、310からの出力を前記フラグレジスタ324の値に応じた切替えるマルチプレクサ、314前記レジスタ311、312からの出力を前記フラグレジスタ308の値に応じて切替えるマルチプレクサである。

315は前記レジスタ302の出力値 P と前記レジスタ304の出力値 C と前記マルチプレクサ313の出力値 d_1 又は d_1' を入力として、計算するべき乗剰余計算回路である。

を行った場合は、 a_1' 又は a_2' の乗法的逆元 a_1' 又は a_2' を計算する。

次に、中国剰余定理を用いて

$$M = x \pmod{P} \quad (x = a_1 \text{ 又は } a_1')$$

$$M = y \pmod{Q} \quad (y = a_2 \text{ 又は } a_2')$$

を解いて M を求めることができる。

第3図は、第2の実施例を示すブロック図である。同図において、301は指数 D をセットするレジスタ、302は素数 P をセットするレジスタ、303は素数 Q をセットするレジスタ、304は被べき乗数 C をセットするレジスタである。

305は指数 $d_1 (= D \pmod{P-1})$ 、指数 $d_1' (= (P-1) - D \pmod{P-1})$ 、指数 $d_2 (= D \pmod{Q-1})$ 、指数 $d_2' (= (Q-1) - D \pmod{Q-1})$ を計算する回路、306は前記 d_1 、 d_1' 、 d_2 、 d_2' 計算回路305からの出力を後述のレジスタ309、310、311、312へ切替えるマルチプレクサである。

309は指数 d_1 をセットするレジスタ、31

316は前記レジスタ303の出力値 Q と前記レジスタ304の出力値 C と前記マルチプレクサ314の出力値 d_2 又は d_2' を入力として計算するべき乗剰余計算回路である。

317は前記べき乗剰余計算回路315からの出力を前記フラグレジスタ324に“1”がたっていたら後述する乗法的逆元計算回路319に出力し、それ以外は後述するマルチプレクサ321に出力するデマルチプレクサである。

318は前記べき乗剰余計算回路316からの出力を前記フラグレジスタ308に“1”がたっていたら後述する乗法的逆元計算回路320に出力し、それ以外は後述するマルチプレクサ322に出力するデマルチプレクサである。

319は前記デマルチプレクサ317の出力値 a_1' と前記レジスタ302の出力値 P を入力として、 $a_1' \cdot a_1' \equiv 1 \pmod{P}$ となる a_1' を計算する乗法的逆元計算回路である。

320は前記デマルチプレクサ318の出力値 a_2' と前記レジスタ303の出力値 Q を入力と

して、 $a \cdot 2^i \cdot a \cdot 2^i \equiv 1 \pmod Q$ となる $a \cdot 2^i$ を計算する乗法的逆元計算回路である。

321は前記フラグレジスタ324に“1”がたっている場合は前記乗法的逆元319の計算回路からの出力に切替え、それ以外の場合は前記デマルチプレクサ317からの出力に切替えるデマルチプレクサである。

322は前記フラグレジスタ308に“1”がたっている場合は前記乗法的逆元の計算回路320からの出力に切替え、それ以外の場合は前記デマルチプレクサ318からの出力に切替えるデマルチプレクサである。

323は前記マルチプレクサ321、322からの出力から復号結果Mを求める中国剰余定理計算回路である。

〔発明の効果〕

以上説明したように、本発明によれば、素数Pを法としたべき乗剰余計算において、指数Dのかわりに $D' (= (P-1) - d)$ を指数としてべき乗剰余計算を行う場合、べき乗剰余計算の乗除

算回数が常に減少し、とくにQuisquaterの方式を使ってRSA暗号の復号化処理をする場合、本方式を組合わせて用いることにより更に高速に復号処理を行うことができる。

4. 図面の簡単な説明

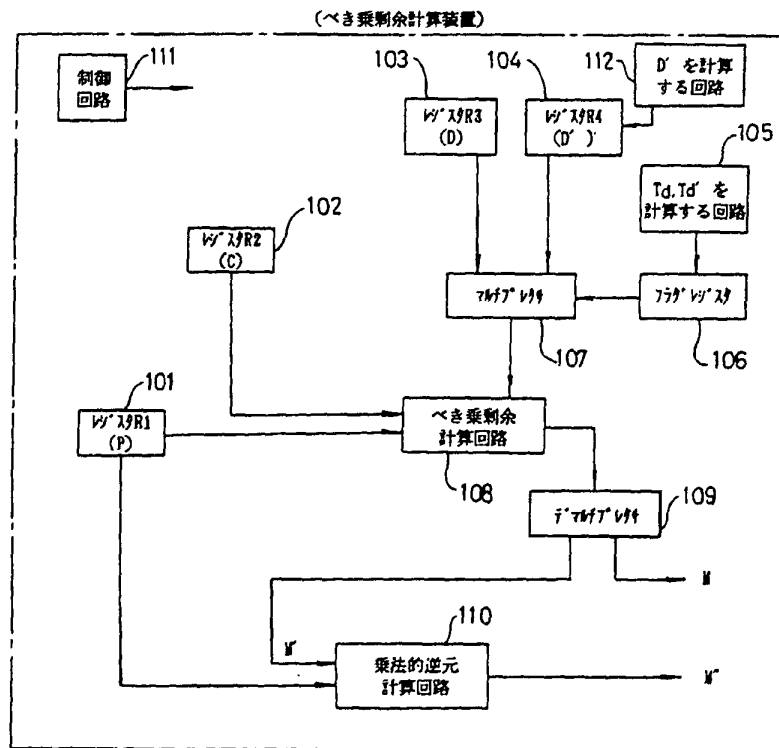
第1図は、本発明における第1の実施例のブロック図、第2図は同実施例の処理手順を示すフローチャート、第3図は第2の実施例のブロック図、第4図は従来のRSA暗号の復号装置のべき乗剰余計算のフローチャートである。

108…べき乗剰余計算回路

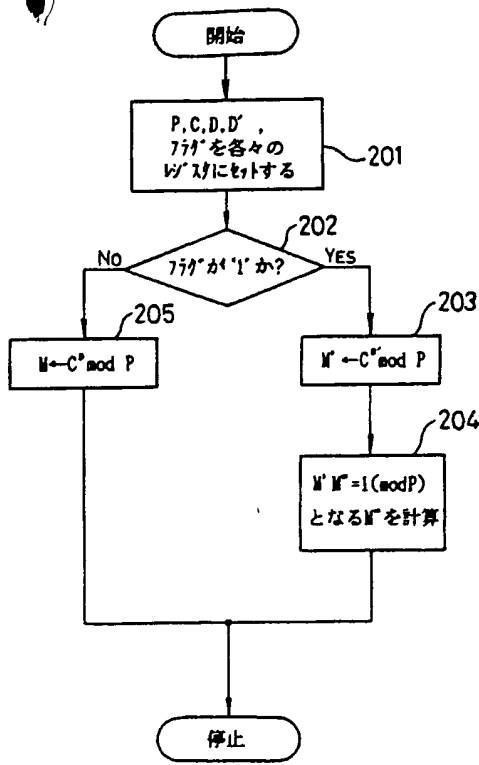
110…乗法的逆元計算回路

112… D' を計算する回路

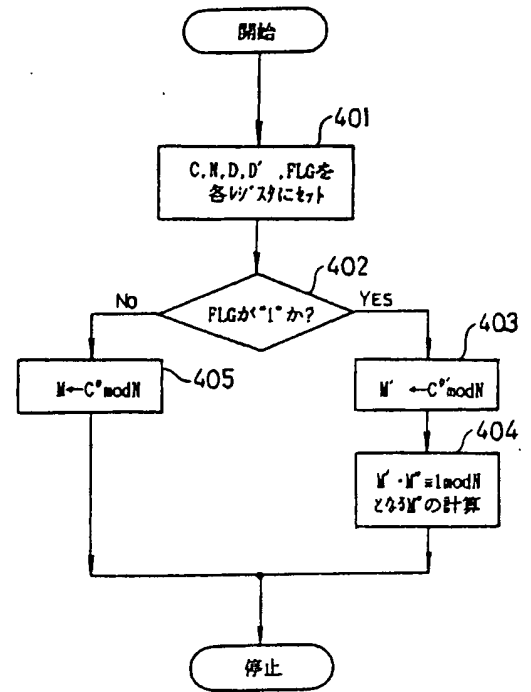
代理人弁理士 三好秀和



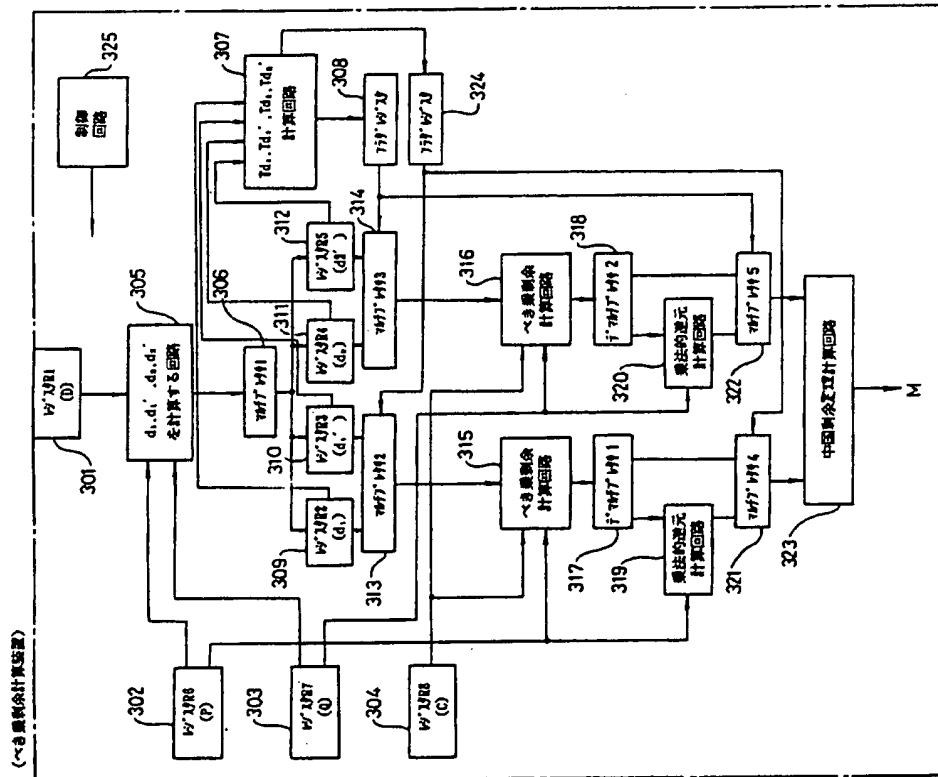
第1図



第 2 図



第 4 図



第 3 図